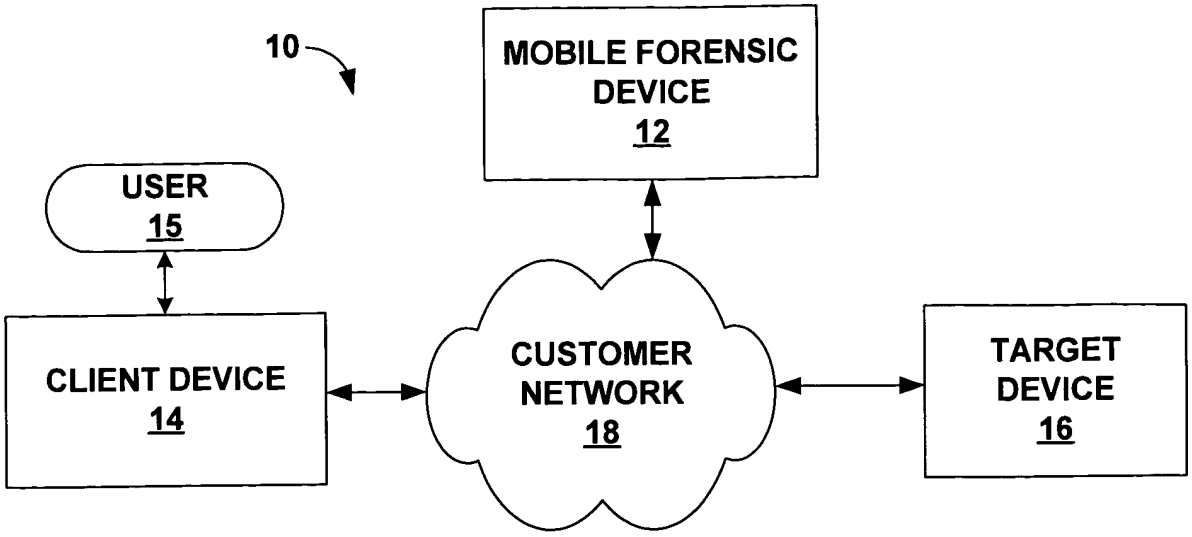

10
MOBILE FORENSIC DEVICE 12
USER 15
CLIENT DEVICE 14
CUSTOMER NETWORK 18
TARGET DEVICE 16

FIG. 1

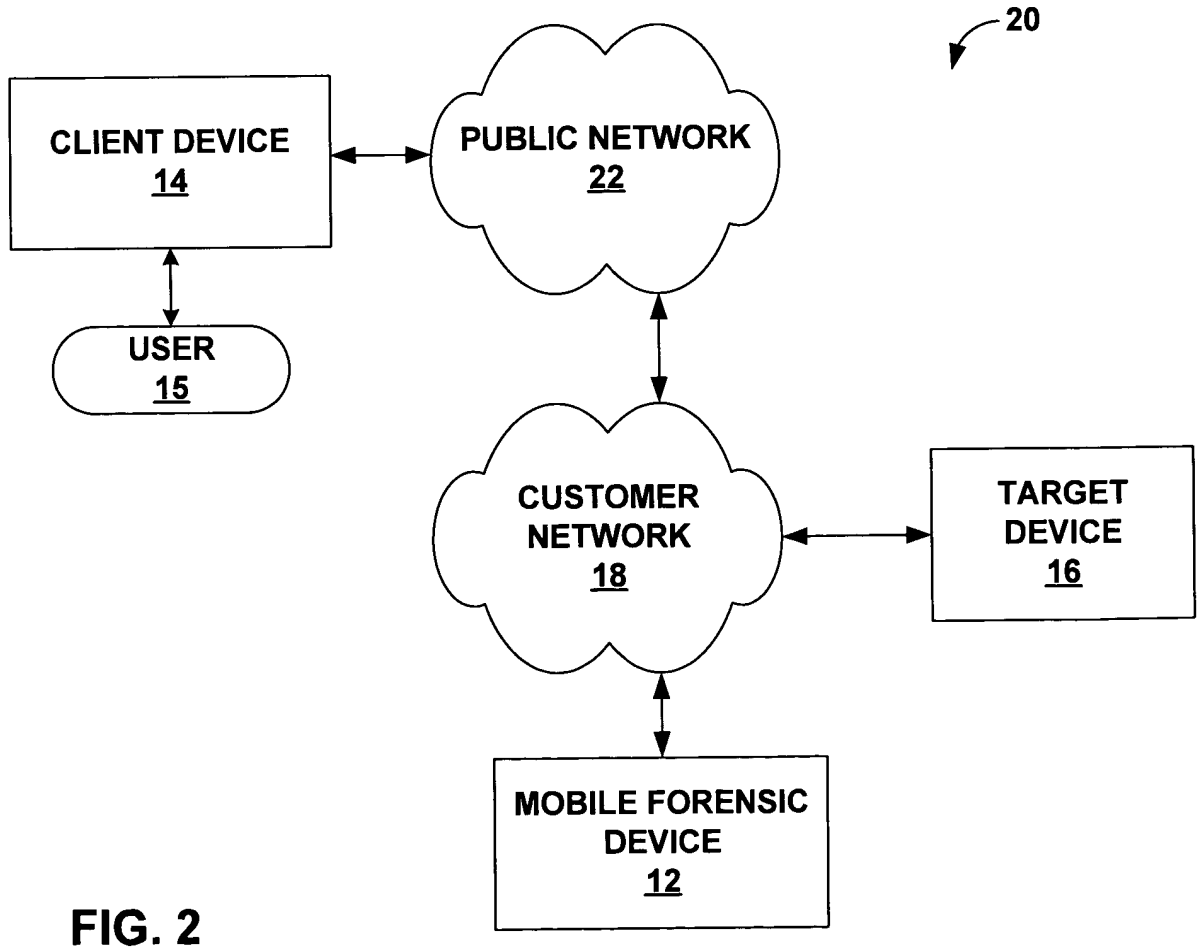

20
CLIENT DEVICE 14
PUBLIC NETWORK 22
USER 15
CUSTOMER NETWORK 18
TARGET DEVICE 16
MOBILE FORENSIC DEVICE 12

FIG. 2

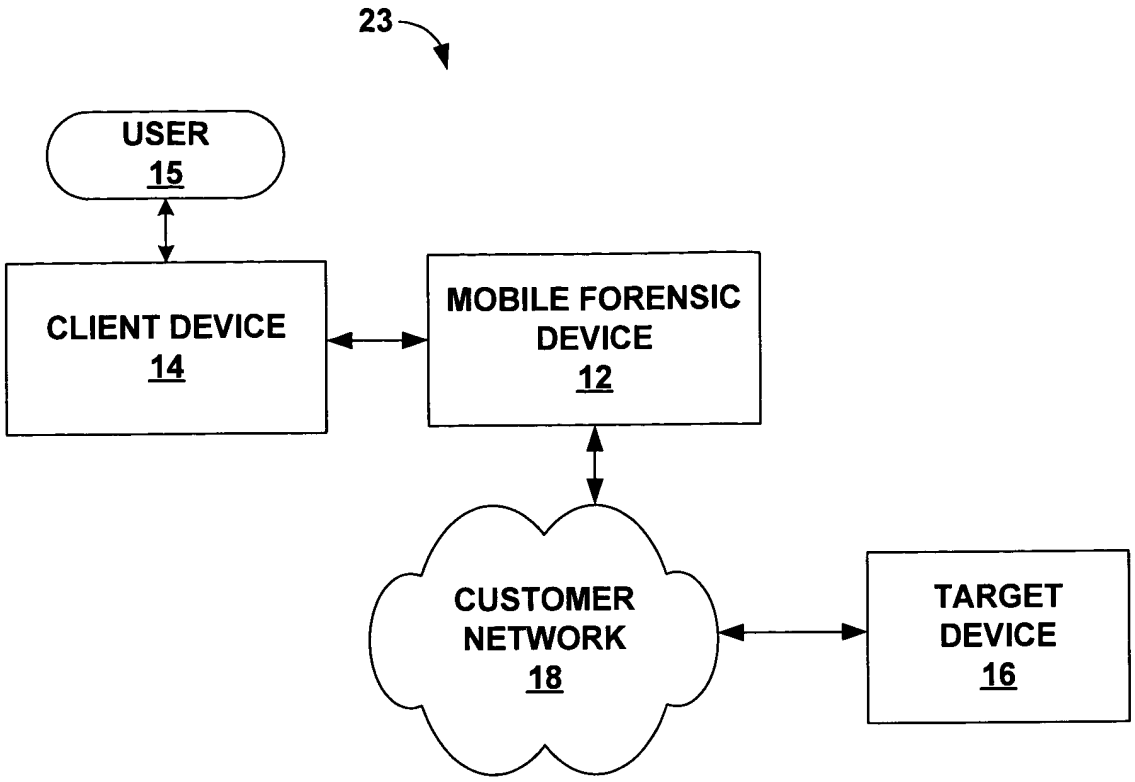

23
USER
15
CLIENT DEVICE
14
MOBILE FORENSIC
DEVICE
12
CUSTOMER
NETWORK
18
TARGET
DEVICE
16

FIG. 3

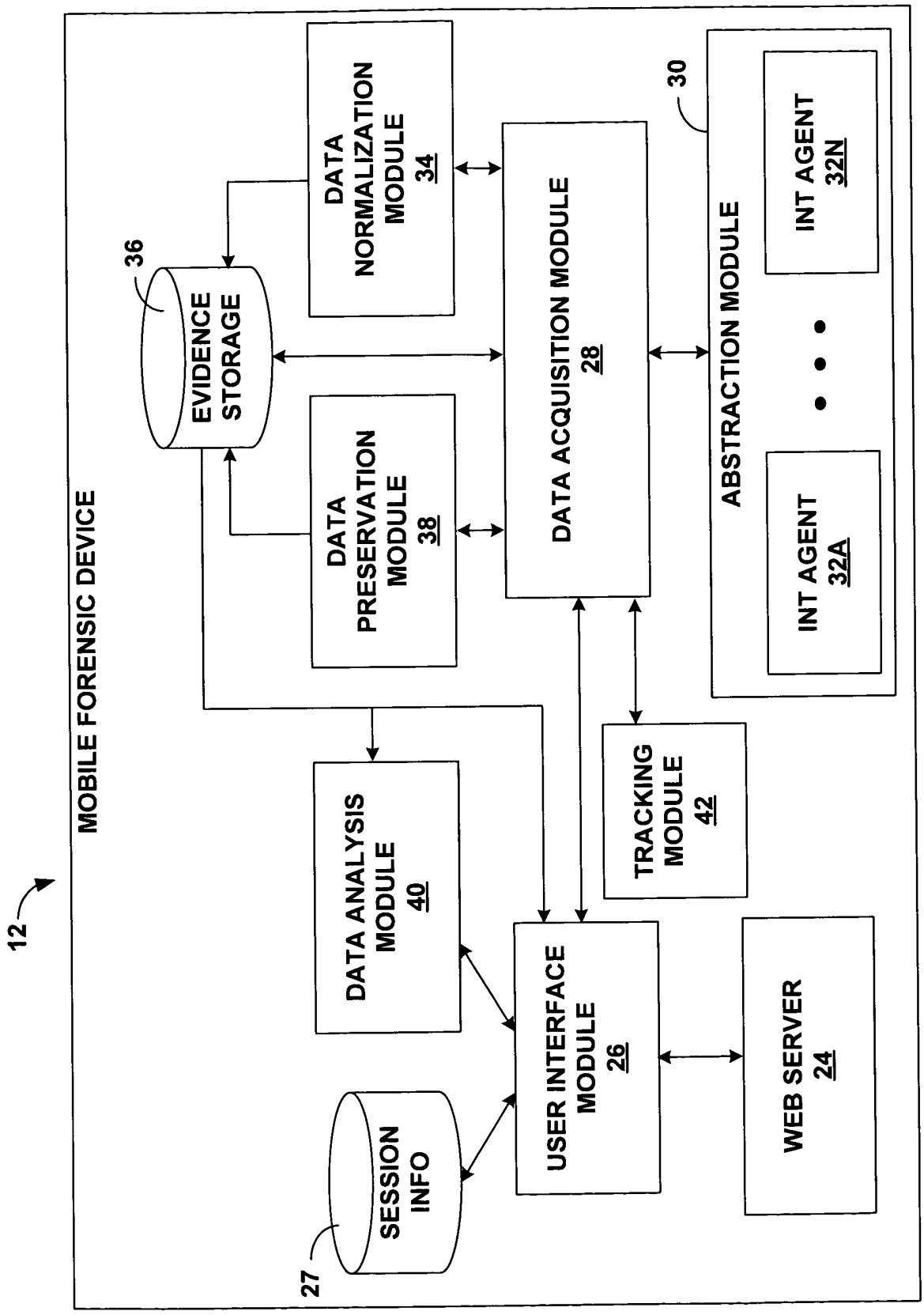

12
MOBILE FORENSIC DEVICE
DATA NORMALIZATION MODULE 34
36
EVIDENCE STORAGE
DATA PRESERVATION MODULE 38
DATA ACQUISITION MODULE 28
30
ABSTRACTION MODULE
INT AGENT 32N
INT AGENT 32A
DATA ANALYSIS MODULE 40
TRACKING MODULE 42
USER INTERFACE MODULE 26
WEB SERVER 24
27
SESSION INFO

FIG. 4

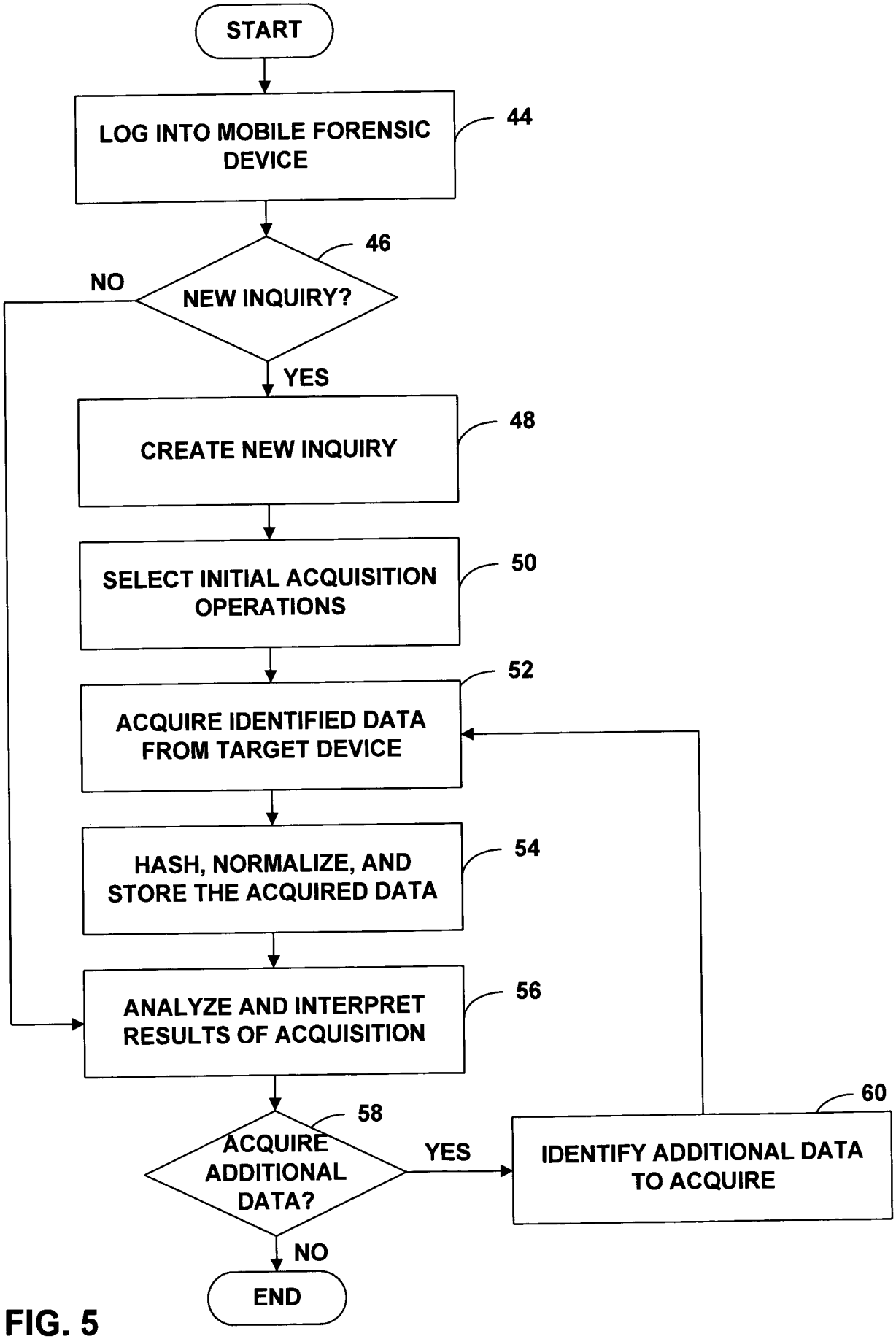

START
LOG INTO MOBILE FORENSIC DEVICE
44
46
NEW INQUIRY?
NO
YES
CREATE NEW INQUIRY
48
SELECT INITIAL ACQUISITION OPERATIONS
50
ACQUIRE IDENTIFIED DATA FROM TARGET DEVICE
52
HASH, NORMALIZE, AND STORE THE ACQUIRED DATA
54
ANALYZE AND INTERPRET RESULTS OF ACQUISITION
56
ACQUIRE ADDITIONAL DATA?
58
YES
IDENTIFY ADDITIONAL DATA TO ACQUIRE
60
NO
END

FIG. 5

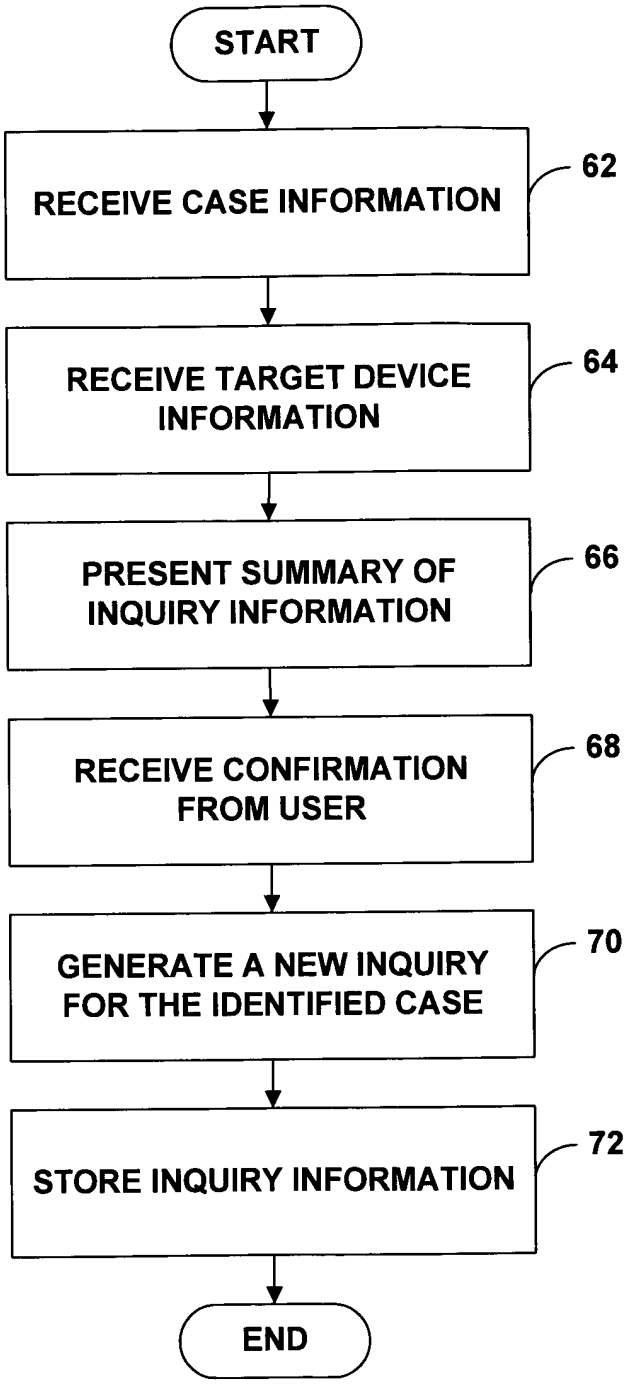

START
RECEIVE CASE INFORMATION
62
RECEIVE TARGET DEVICE INFORMATION
64
PRESENT SUMMARY OF INQUIRY INFORMATION
66
RECEIVE CONFIRMATION FROM USER
68
GENERATE A NEW INQUIRY FOR THE IDENTIFIED CASE
70
STORE INQUIRY INFORMATION
72
END

FIG. 6

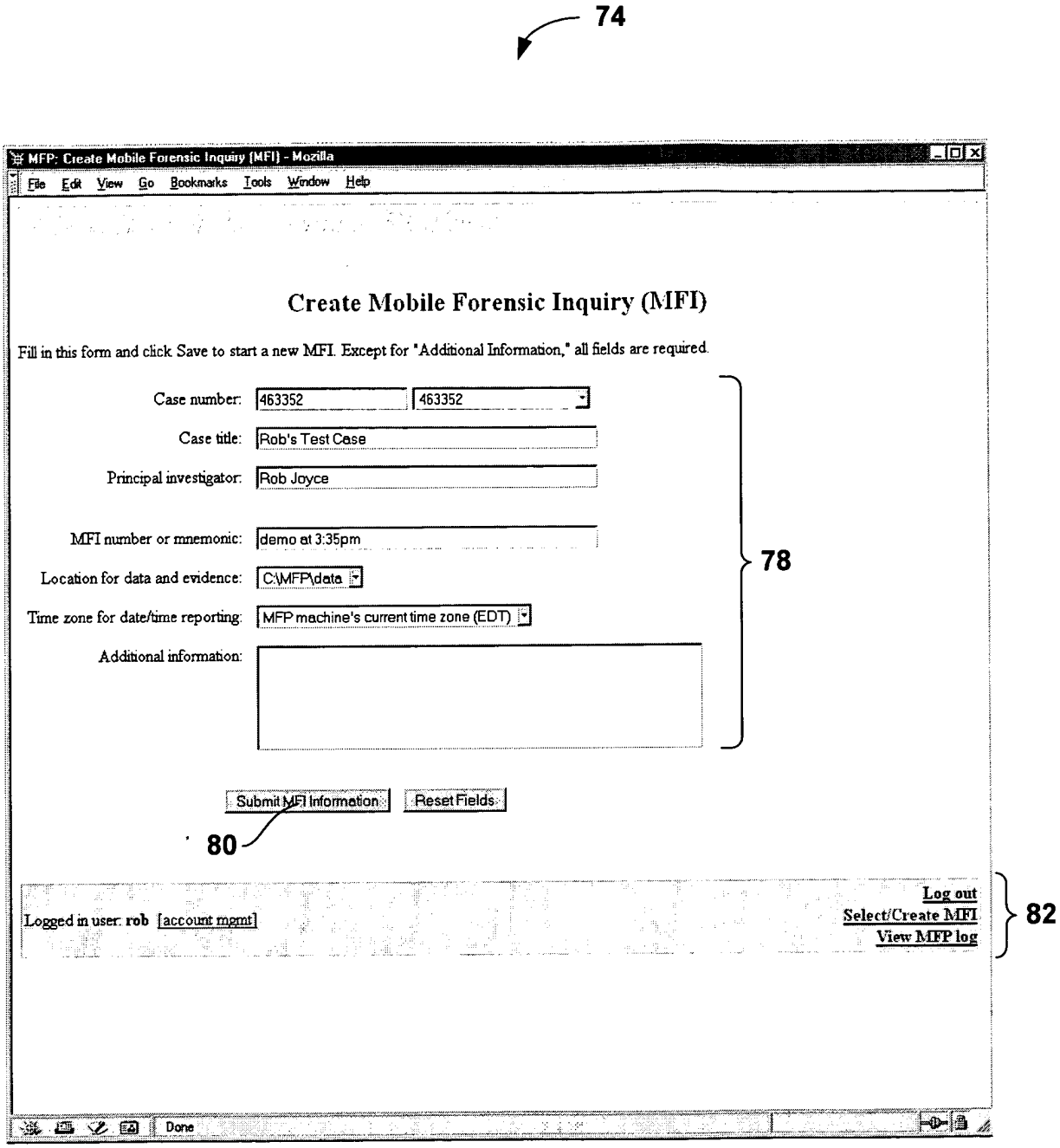

74
MFP: Create Mobile Forensic Inquiry (MFI) - Mozilla
File Edit View Go Bookmarks Tools Window Help
Create Mobile Forensic Inquiry (MFI)
Fill in this form and click Save to start a new MFI. Except for "Additional Information," all fields are required.
Case number: 463352 463352
Case title: Rob's Test Case
Principal investigator: Rob Joyce
MFI number or mnemonic: demo at 3:35pm
Location for data and evidence: C:\MFP\data
Time zone for date/time reporting: MFP machine's current time zone (EDT)
Additional information:
78
Submit MFI Information
Reset Fields
80
Logged in user: rob [account mgmt]
Log out
Select/Create MFI
View MFP log
82
Done

FIG. 7

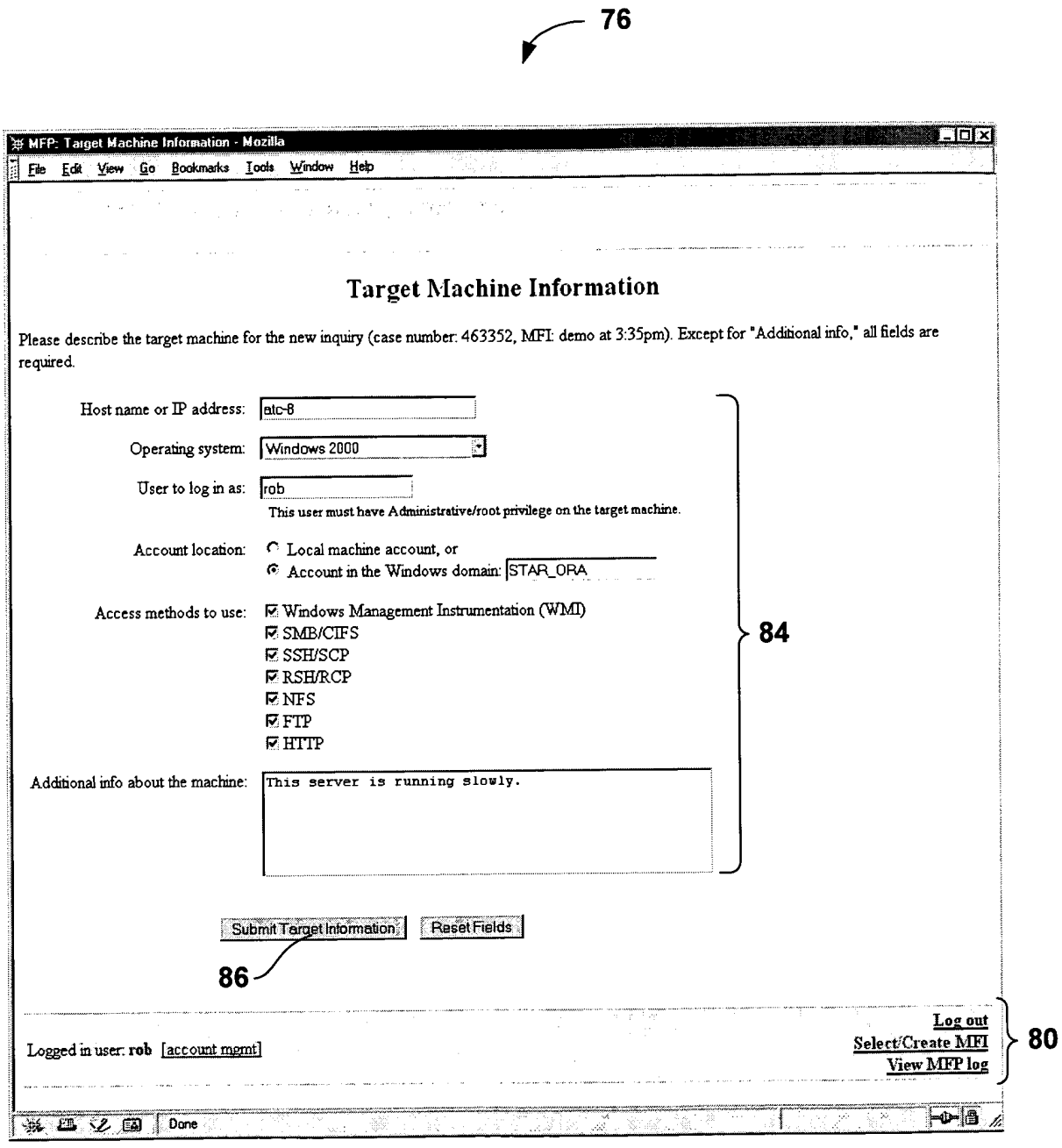

76
MFP: Target Machine Information - Mozilla
File Edit View Go Bookmarks Tools Window Help
Target Machine Information
Please describe the target machine for the new inquiry (case number: 463352, MFI: demo at 3:35pm). Except for "Additional info," all fields are required.
Host name or IP address: atc-8
Operating system: Windows 2000
User to log in as: rob
This user must have Administrative/root privilege on the target machine.
Account location: Local machine account, or
Account in the Windows domain: STAR_ORA
Access methods to use: Windows Management Instrumentation (WMI)
SMB/CIFS
SSH/SCP
RSH/RCP
NFS
FTP
HTTP
Additional info about the machine: This server is running slowly.
84
Submit Target Information
Reset Fields
86
Logged in user: rob [account mgmt]
Log out
Select/Create MFI
View MFP log
80
Done

FIG. 8

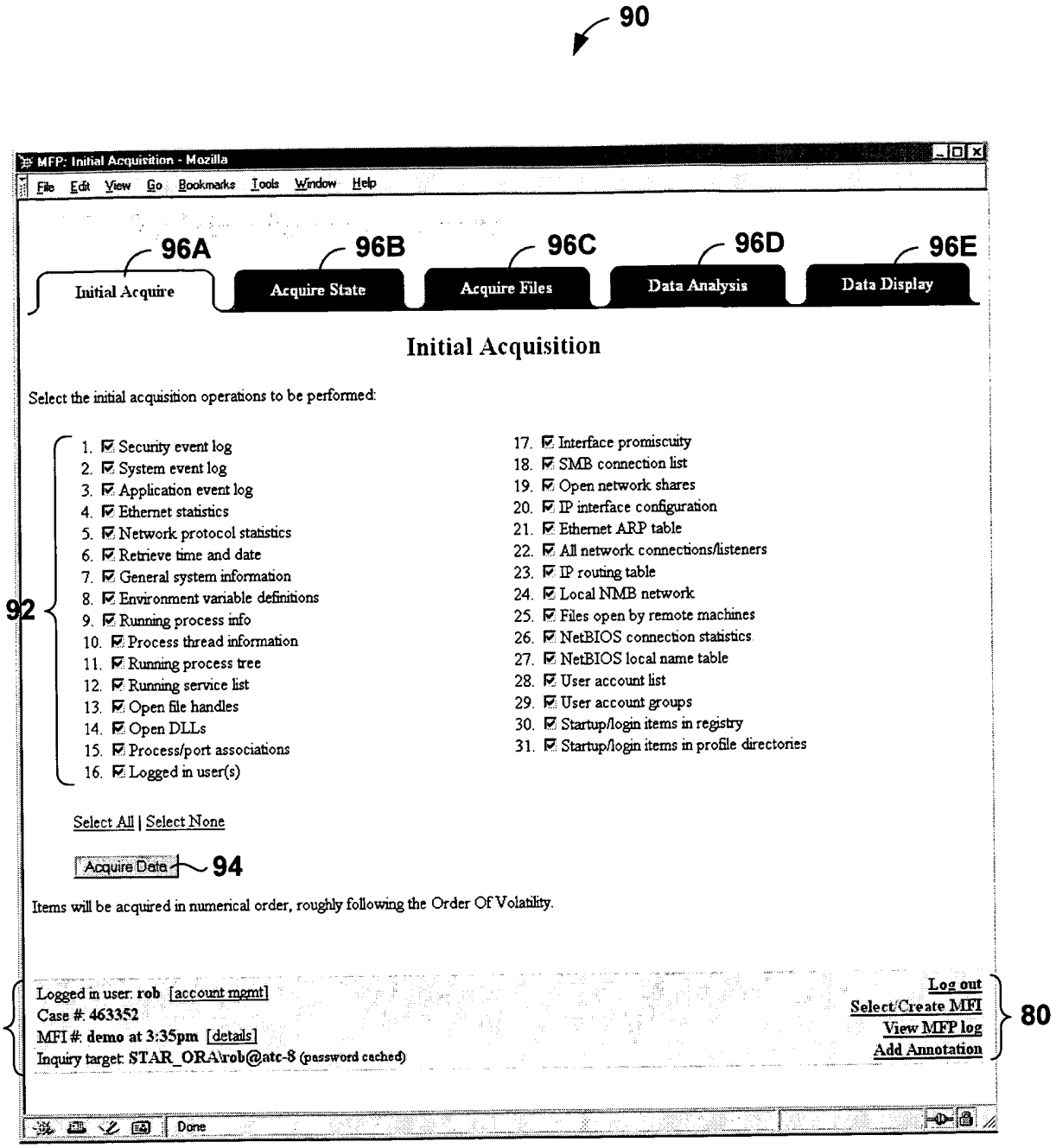

90
MFP: Initial Acquisition - Mozilla
File Edit View Go Bookmarks Tools Window Help
96A
96B
96C
96D
96E
Initial Acquire
Acquire State
Acquire Files
Data Analysis
Data Display
Initial Acquisition
Select the initial acquisition operations to be performed:
92
1. Security event log
2. System event log
3. Application event log
4. Ethernet statistics
5. Network protocol statistics
6. Retrieve time and date
7. General system information
8. Environment variable definitions
9. Running process info
10. Process thread information
11. Running process tree
12. Running service list
13. Open file handles
14. Open DLLs
15. Process/port associations
16. Logged in user(s)
17. Interface promiscuity
18. SMB connection list
19. Open network shares
20. IP interface configuration
21. Ethernet ARP table
22. All network connections/listeners
23. IP routing table
24. Local NMB network
25. Files open by remote machines
26. NetBIOS connection statistics
27. NetBIOS local name table
28. User account list
29. User account groups
30. Startup/login items in registry
31. Startup/login items in profile directories
Select All | Select None
Acquire Data
94
Items will be acquired in numerical order, roughly following the Order Of Volatility.
98
Logged in user: rob [account mgmt]
Case #: 463352
MFI #: demo at 3:35pm [details]
Inquiry target: STAR_ORA\rob@atc-8 (password cached)
Log out
Select/Create MFI
View MFP log
Add Annotation
80
Done

FIG. 9

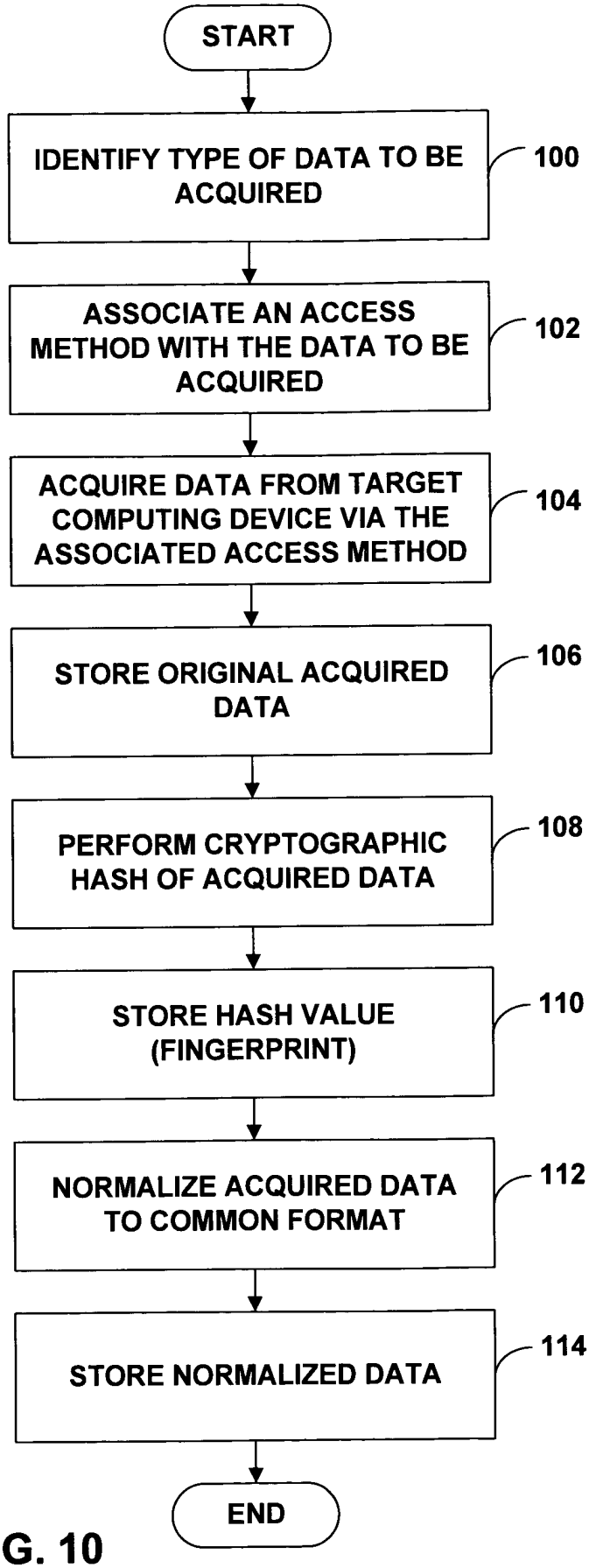

START
IDENTIFY TYPE OF DATA TO BE ACQUIRED
100
ASSOCIATE AN ACCESS METHOD WITH THE DATA TO BE ACQUIRED
102
ACQUIRE DATA FROM TARGET COMPUTING DEVICE VIA THE ASSOCIATED ACCESS METHOD
104
STORE ORIGINAL ACQUIRED DATA
106
PERFORM CRYPTOGRAPHIC HASH OF ACQUIRED DATA
108
STORE HASH VALUE (FINGERPRINT)
110
NORMALIZE ACQUIRED DATA TO COMMON FORMAT
112
STORE NORMALIZED DATA
114
END

FIG. 10

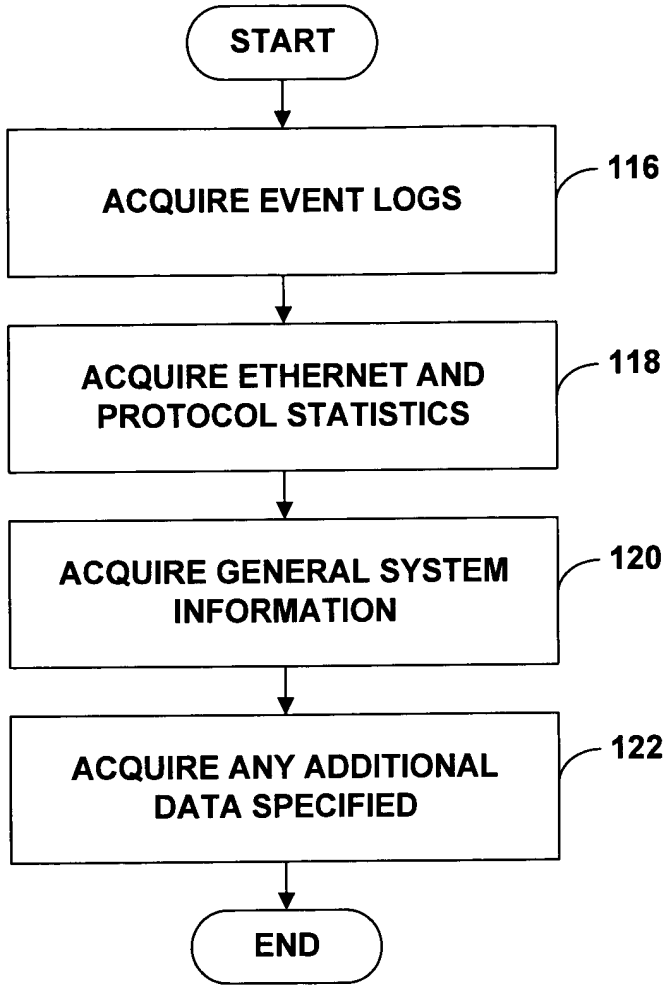
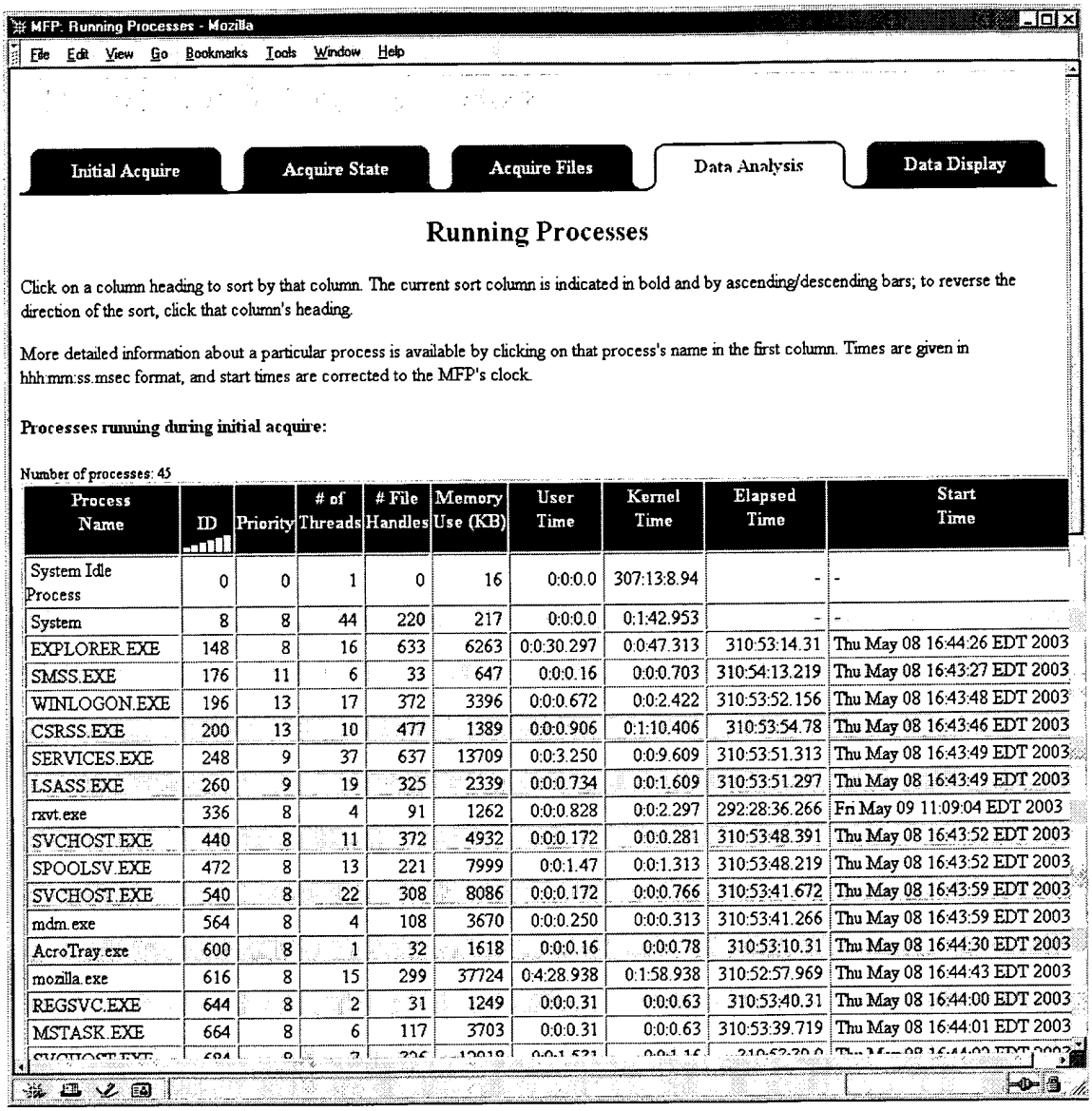

START
ACQUIRE EVENT LOGS
116
ACQUIRE ETHERNET AND PROTOCOL STATISTICS
118
ACQUIRE GENERAL SYSTEM INFORMATION
120
ACQUIRE ANY ADDITIONAL DATA SPECIFIED
122
END

FIG. 11

126



Running Processes

Click on a column heading to sort by that column. The current sort column is indicated in bold and by ascending/descending bars; to reverse the direction of the sort, click that column's heading.

More detailed information about a particular process is available by clicking on that process's name in the first column. Times are given in hhh:mm:ss.msec format, and start times are corrected to the MFP's clock.

Processes running during initial acquire:

Number of processes: 45

Process Name	ID	Priority	# of Threads	# File Handles	Memory Use (KB)	User Time	Kernel Time	Elapsed Time	Start Time
System Idle Process	0	0	1	0	16	0:0:0.0	307:13:8.94	-	-
System	8	8	44	220	217	0:0:0.0	0:1:42.953	-	-
EXPLORER.EXE	148	8	16	633	6263	0:0:30.297	0:0:47.313	310:53:14.31	Thu May 08 16:44:26 EDT 2003
SMSS.EXE	176	11	6	33	647	0:0:0.16	0:0:0.703	310:54:13.219	Thu May 08 16:43:27 EDT 2003
WINLOGON.EXE	196	13	17	372	3396	0:0:0.672	0:0:2.422	310:53:52.156	Thu May 08 16:43:48 EDT 2003
CSRSS.EXE	200	13	10	477	1389	0:0:0.906	0:1:10.406	310:53:54.78	Thu May 08 16:43:46 EDT 2003
SERVICES.EXE	248	9	37	637	13709	0:0:3.250	0:0:9.609	310:53:51.313	Thu May 08 16:43:49 EDT 2003
LSASS.EXE	260	9	19	325	2339	0:0:0.734	0:0:1.609	310:53:51.297	Thu May 08 16:43:49 EDT 2003
rxvt.exe	336	8	4	91	1262	0:0:0.828	0:0:2.297	292:28:36.266	Fri May 09 11:09:04 EDT 2003
SVCHOST.EXE	440	8	11	372	4932	0:0:0.172	0:0:0.281	310:53:48.391	Thu May 08 16:43:52 EDT 2003
SPOOLSV.EXE	472	8	13	221	7999	0:0:1.47	0:0:1.313	310:53:48.219	Thu May 08 16:43:52 EDT 2003
SVCHOST.EXE	540	8	22	308	8086	0:0:0.172	0:0:0.766	310:53:41.672	Thu May 08 16:43:59 EDT 2003
mdm.exe	564	8	4	108	3670	0:0:0.250	0:0:0.313	310:53:41.266	Thu May 08 16:43:59 EDT 2003
AcroTray.exe	600	8	1	32	1618	0:0:0.16	0:0:0.78	310:53:10.31	Thu May 08 16:44:30 EDT 2003
mozilla.exe	616	8	15	299	37724	0:4:28.938	0:1:58.938	310:52:57.969	Thu May 08 16:44:43 EDT 2003
REGSVC.EXE	644	8	2	31	1249	0:0:0.31	0:0:0.63	310:53:40.31	Thu May 08 16:44:00 EDT 2003
MSTASK.EXE	664	8	6	117	3703	0:0:0.31	0:0:0.63	310:53:39.719	Thu May 08 16:44:01 EDT 2003

FIG. 12

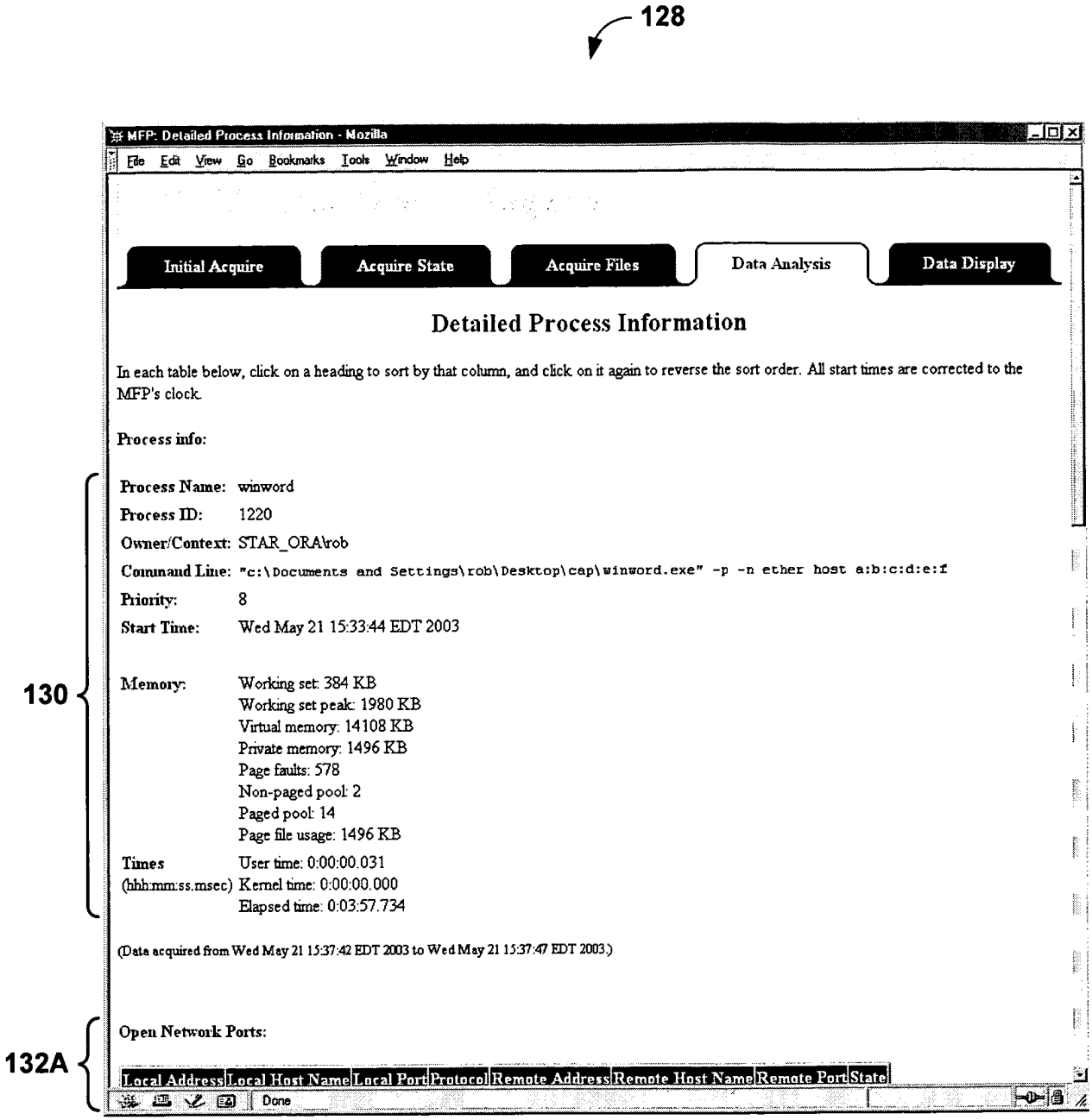

128
MFP: Detailed Process Information - Mozilla
File Edit View Go Bookmarks Tools Window Help
Initial Acquire
Acquire State
Acquire Files
Data Analysis
Data Display
Detailed Process Information
In each table below, click on a heading to sort by that column, and click on it again to reverse the sort order. All start times are corrected to the MFP's clock.
Process info:
Process Name: winword
Process ID: 1220
Owner/Context: STAR_ORA\rob
Command Line: "c:\Documents and Settings\rob\Desktop\cap\winword.exe" -p -n ether host a:b:c:d:e:f
Priority: 8
Start Time: Wed May 21 15:33:44 EDT 2003
Memory: Working set: 384 KB
Working set peak: 1980 KB
Virtual memory: 14108 KB
Private memory: 1496 KB
Page faults: 578
Non-paged pool: 2
Paged pool: 14
Page file usage: 1496 KB
Times (hhh:mm:ss.msec) User time: 0:00:00.031
Kernel time: 0:00:00.000
Elapsed time: 0:03:57.734
(Data acquired from Wed May 21 15:37:42 EDT 2003 to Wed May 21 15:37:47 EDT 2003.)
Open Network Ports:
Local Address Local Host Name Local Port Protocol Remote Address Remote Host Name Remote Port State
Done
130
132A

FIG. 13A

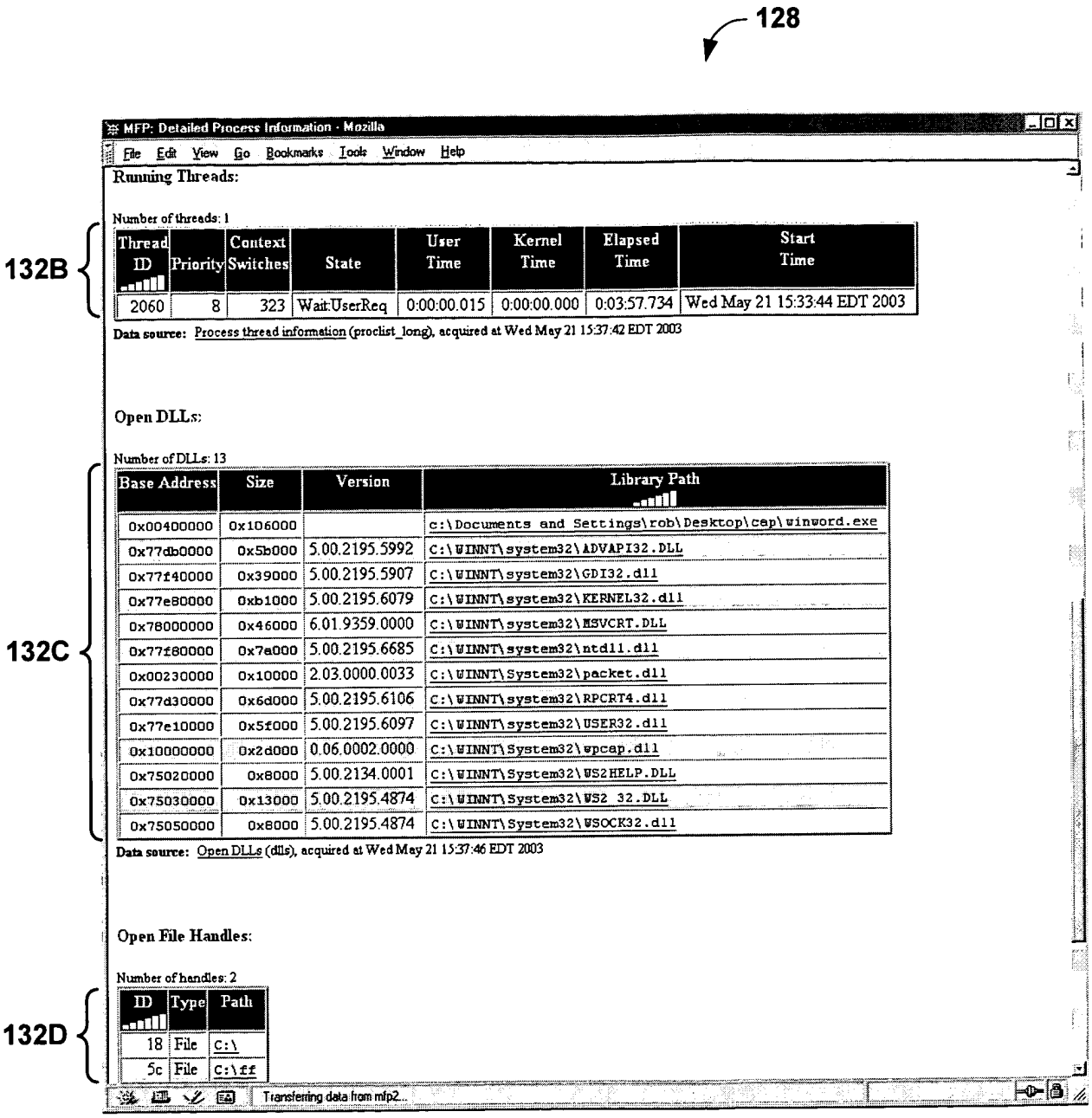

128
MFP: Detailed Process Information - Mozilla
File Edit View Go Bookmarks Tools Window Help
Running Threads:
Number of threads: 1
132B
Thread ID | Priority | Context Switches | State | User Time | Kernel Time | Elapsed Time | Start Time
2060 | 8 | 323 | Wait:UserReq | 0:00:00.015 | 0:00:00.000 | 0:03:57.734 | Wed May 21 15:33:44 EDT 2003
Data source: Process thread information (proclist_long), acquired at Wed May 21 15:37:42 EDT 2003
Open DLLs:
Number of DLLs: 13
132C
Base Address | Size | Version | Library Path
0x00400000 | 0x106000 | | c:\Documents and Settings\rob\Desktop\cap\winword.exe
0x77db0000 | 0x5b000 | 5.00.2195.5992 | C:\WINNT\system32\ADVAPI32.DLL
0x77f40000 | 0x39000 | 5.00.2195.5907 | C:\WINNT\system32\GDI32.dll
0x77e80000 | 0xb1000 | 5.00.2195.6079 | C:\WINNT\system32\KERNEL32.dll
0x78000000 | 0x46000 | 6.01.9359.0000 | C:\WINNT\system32\MSVCRT.DLL
0x77f80000 | 0x7a000 | 5.00.2195.6685 | C:\WINNT\system32\ntdll.dll
0x00230000 | 0x10000 | 2.03.0000.0033 | C:\WINNT\System32\packet.dll
0x77d30000 | 0x6d000 | 5.00.2195.6106 | C:\WINNT\system32\RPCRT4.dll
0x77e10000 | 0x5f000 | 5.00.2195.6097 | C:\WINNT\system32\USER32.dll
0x10000000 | 0x2d000 | 0.06.0002.0000 | C:\WINNT\System32\wpcap.dll
0x75020000 | 0x8000 | 5.00.2134.0001 | C:\WINNT\System32\WS2HELP.DLL
0x75030000 | 0x13000 | 5.00.2195.4874 | C:\WINNT\System32\WS2_32.DLL
0x75050000 | 0x8000 | 5.00.2195.4874 | C:\WINNT\System32\WSOCK32.dll
Data source: Open DLLs (dlls), acquired at Wed May 21 15:37:46 EDT 2003
Open File Handles:
Number of handles: 2
132D
ID | Type | Path
18 | File | C:\
5c | File | C:\ff
Transferring data from mfp2...

FIG. 13B

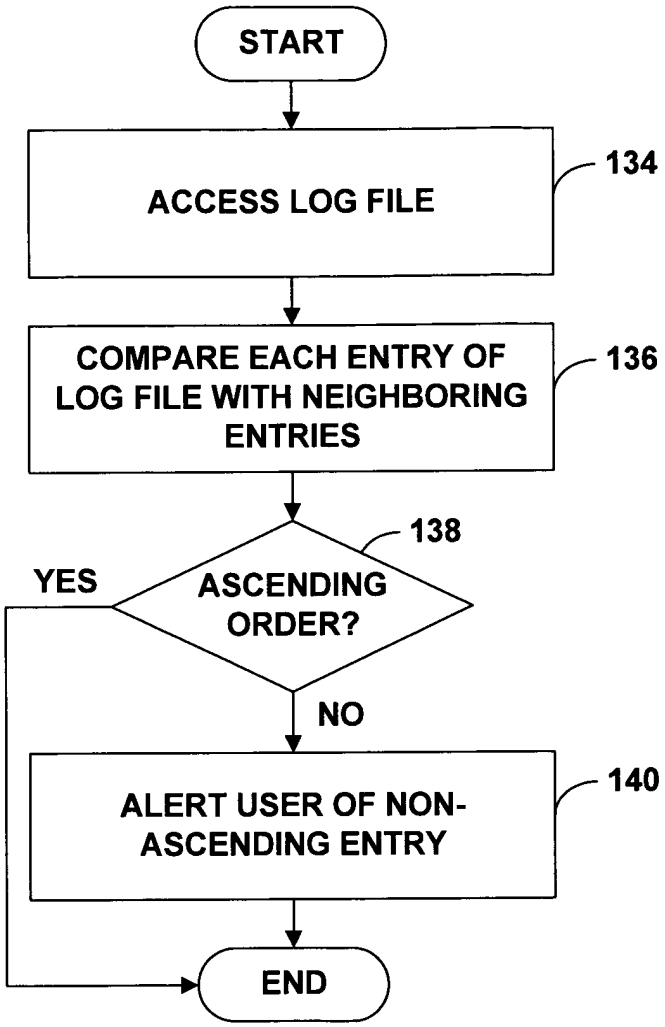

START
ACCESS LOG FILE
134
COMPARE EACH ENTRY OF LOG FILE WITH NEIGHBORING ENTRIES
136
138
YES
ASCENDING ORDER?
NO
ALERT USER OF NON-ASCENDING ENTRY
140
END

FIG. 14

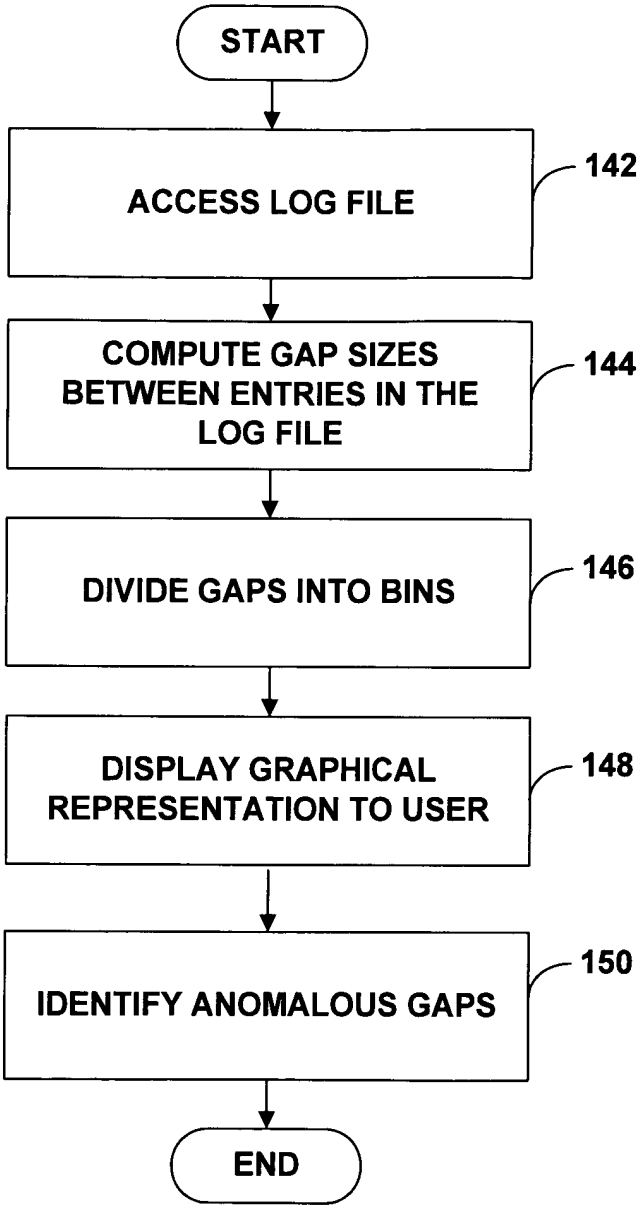

START
ACCESS LOG FILE
142
COMPUTE GAP SIZES BETWEEN ENTRIES IN THE LOG FILE
144
DIVIDE GAPS INTO BINS
146
DISPLAY GRAPHICAL REPRESENTATION TO USER
148
IDENTIFY ANOMALOUS GAPS
150
END

FIG. 15

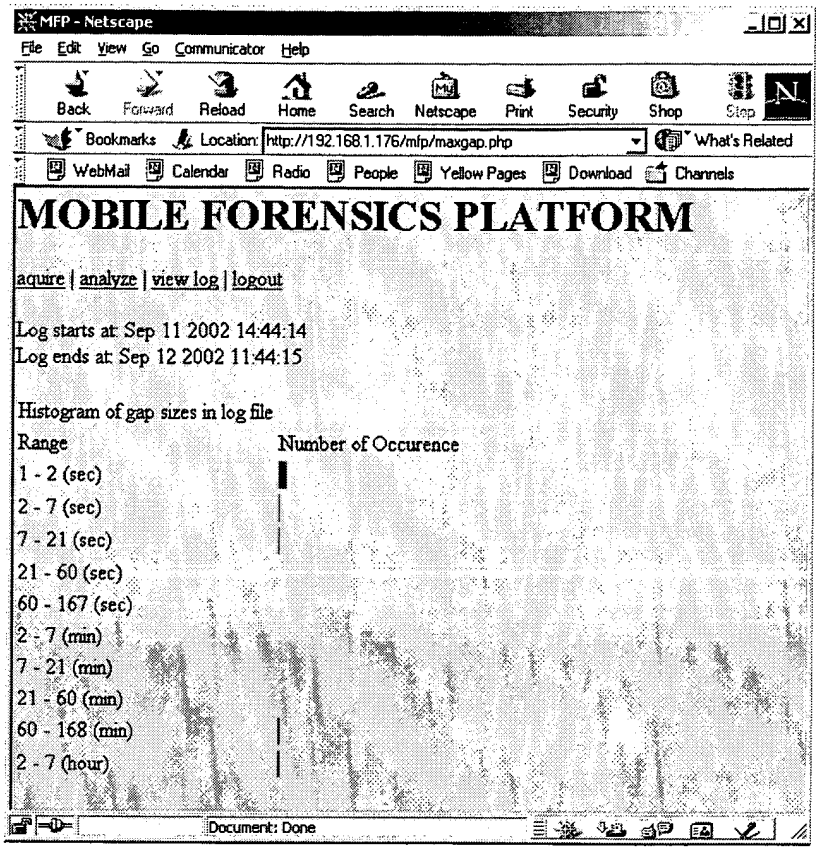

160
MFP - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://192.168.1.176/mfp/maxgap.php What's Related
WebMail Calendar Radio People Yellow Pages Download Channels
MOBILE FORENSICS PLATFORM
aquire | analyze | view log | logout
Log starts at: Sep 11 2002 14:44:14
Log ends at: Sep 12 2002 11:44:15
Histogram of gap sizes in log file
Range
Number of Occurence
1 - 2 (sec)
2 - 7 (sec)
7 - 21 (sec)
21 - 60 (sec)
60 - 167 (sec)
2 - 7 (min)
7 - 21 (min)
21 - 60 (min)
60 - 168 (min)
2 - 7 (hour)
Document: Done

FIG. 16

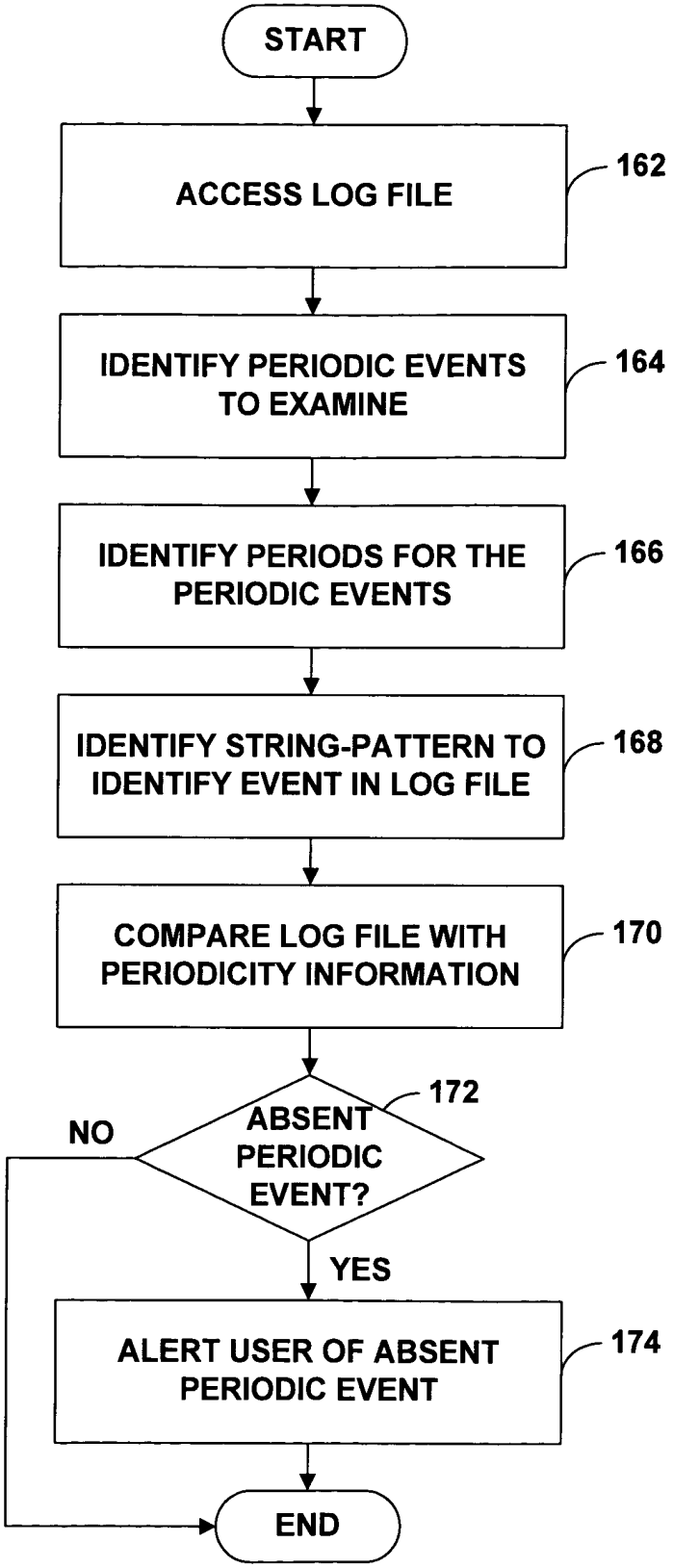

START
ACCESS LOG FILE
162
IDENTIFY PERIODIC EVENTS TO EXAMINE
164
IDENTIFY PERIODS FOR THE PERIODIC EVENTS
166
IDENTIFY STRING-PATTERN TO IDENTIFY EVENT IN LOG FILE
168
COMPARE LOG FILE WITH PERIODICITY INFORMATION
170
ABSENT PERIODIC EVENT?
172
NO
YES
ALERT USER OF ABSENT PERIODIC EVENT
174
END

FIG. 17